



# **Smart Policy - Web Collector**

Version 1.1

Prepared by: "Vincent Le Toux"

Date: 29/05/2014

# Table of Contents

---

## Table of Contents

### Revision History

### Overview

Requirements .....	5
Overview .....	5
Check that a certificate is trusted and found in the user store .....	6
Check that a certificate is trusted by the computer store .....	7
Install asp.net if it is not already installed .....	9

### **Installation**

1a New website installation .....	10
1b Virtual directory installation .....	12
2 Enable the Windows Authentication .....	13
3 Enable kerberos authentication .....	13
4 Configure the SSL settings .....	15

### **User workflow**

### **Troubleshooting**

HTTP Error 403.7 - The client certificate was missing or unrecognized .....	18
---	----

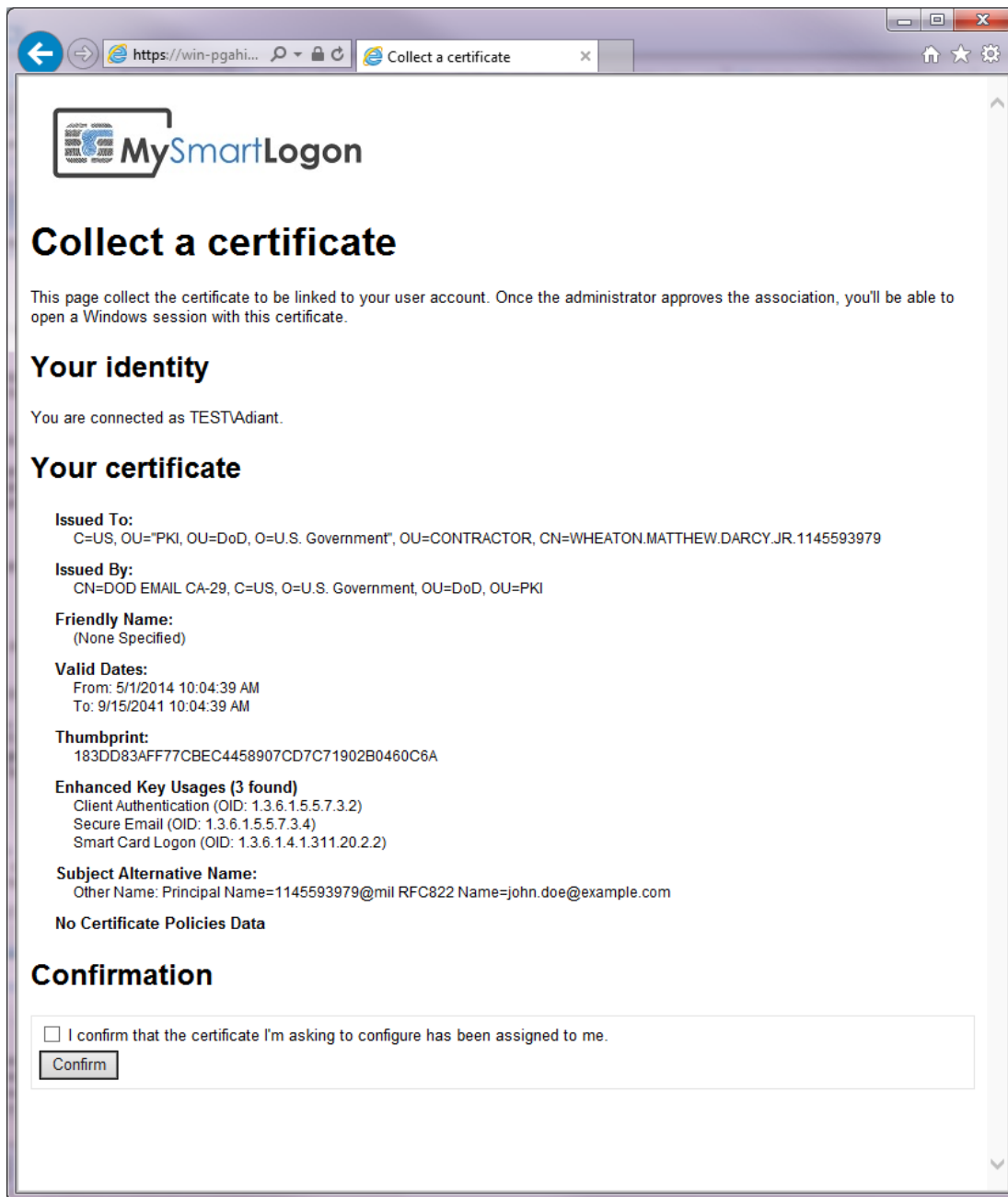


## Overview

---

Smart Policy is a set of tools to integrate existing smart cards into an Active Directory to be able to use them for login.

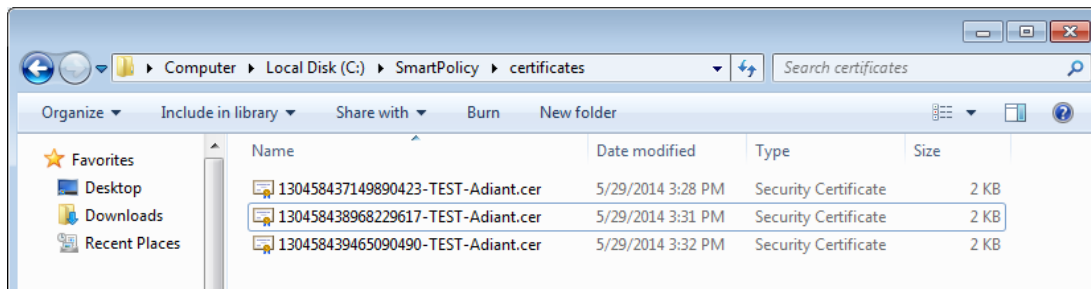
Smart Policy Web Collector is a small web application running on IIS which collects smart card certificates remotely. Once the procedure is completed by the user, the certificates are stored in a directory which can be used for further processing.



The screenshot shows a web browser window with the URL `https://win-pgahi...` and a tab titled "Collect a certificate". The page features the MySmartLogon logo at the top left. Below the logo is the main heading "Collect a certificate" and a paragraph explaining the process: "This page collect the certificate to be linked to your user account. Once the administrator approves the association, you'll be able to open a Windows session with this certificate."

The page is divided into several sections:

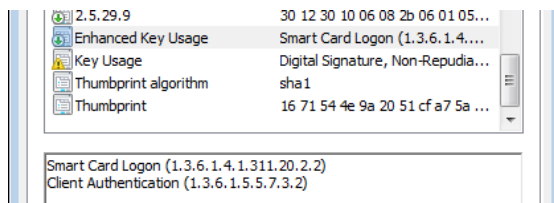
- Your identity**: "You are connected as TEST\Adiant."
- Your certificate**:
  - Issued To:** C=US, OU="PKI, OU=DoD, O=U.S. Government", OU=CONTRACTOR, CN=WHEATON.MATTHEW.DARCY.JR.1145593979
  - Issued By:** CN=DOD EMAIL CA-29, C=US, O=U.S. Government, OU=DoD, OU=PKI
  - Friendly Name:** (None Specified)
  - Valid Dates:** From: 5/1/2014 10:04:39 AM, To: 9/15/2041 10:04:39 AM
  - Thumbprint:** 183DD83AFF77CBEC4458907CD7C71902B0460C6A
  - Enhanced Key Usages (3 found):** Client Authentication (OID: 1.3.6.1.5.5.7.3.2), Secure Email (OID: 1.3.6.1.5.5.7.3.4), Smart Card Logon (OID: 1.3.6.1.4.1.311.20.2.2)
  - Subject Alternative Name:** Other Name: Principal Name=1145593979@mil RFC822 Name=john.doe@example.com
  - No Certificate Policies Data**
- Confirmation**: A checkbox labeled "I confirm that the certificate I'm asking to configure has been assigned to me." followed by a "Confirm" button.



## Requirements

### Overview

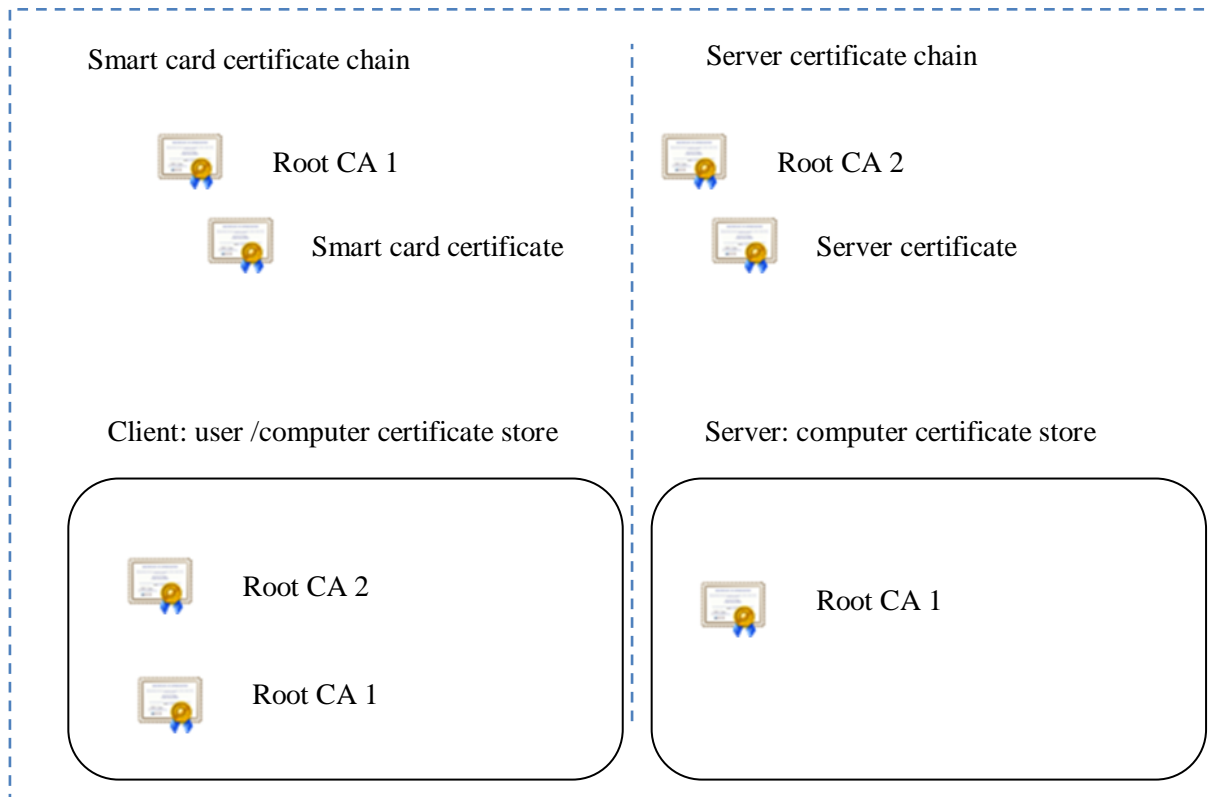
- An IIS webserver with ASP.net with 10MB of free space and connected to the active directory you want to configure.
- A webserver SSL certificate which MAY not be trusted by the browser, typically issued by the Active Directory Certificate Services component
- A smart card with a certificate. This certificate **MUST** be trusted by the browser and the webserver
- The smart certificate **MUST** have the Extended Key Usage "Client Authentication (1.3.6.1.5.5.7.3.2)"



The web collector doesn't work with certificates having the EKU " Smart Card Logon (1.3.6.1.4.1.311.20.2.2)" and which don't have the "Client Authentication" EKU.

The certificate authorities used by the smart card and the webserver can be the same but it is not a requirement.

The following figure describes how the trust requirement can be achieved:

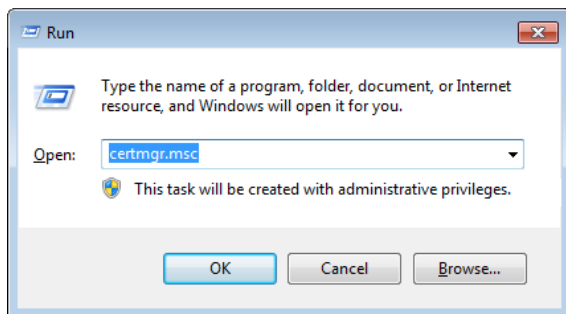


Here is a short procedure to check that the root certificates are trusted

***Check that a certificate is trusted and found in the user store***

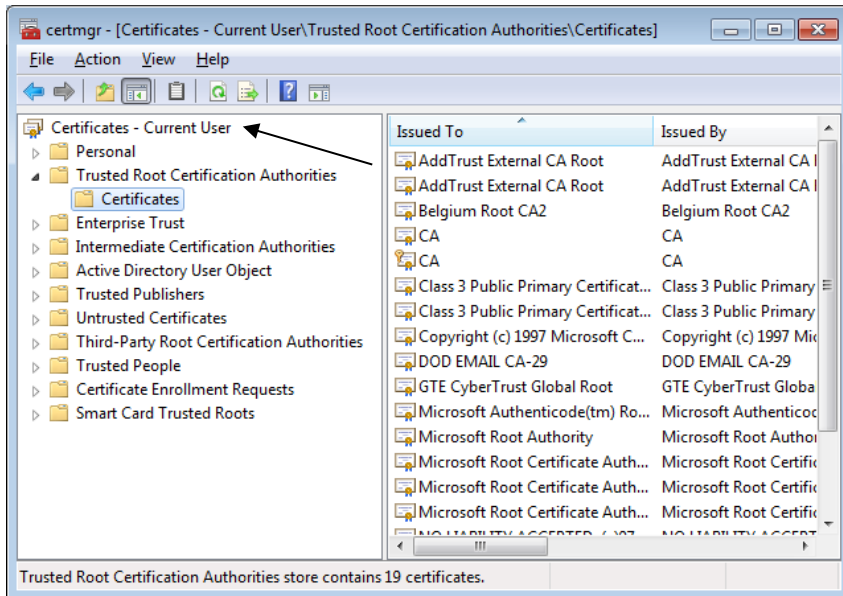
This procedure is used on the browser side.

Type the Windows Key + R. A new dialog is shown. Type "certmgr.msc" and press Enter.



The certificate store dialog appears. Open the "Trusted Root Certification Authorities" folder and check at the right that the certificate appears.

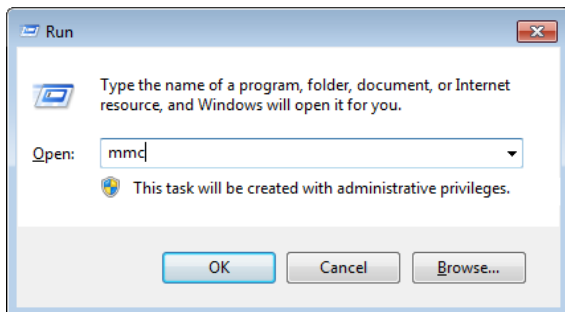
Please pay attention to the mention "Current user"



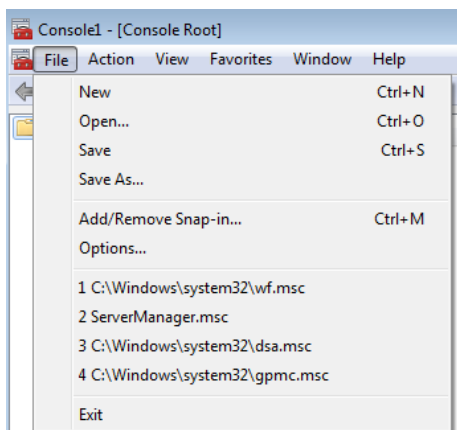
**Check that a certificate is trusted by the computer store**

This procedure is used on the server side.

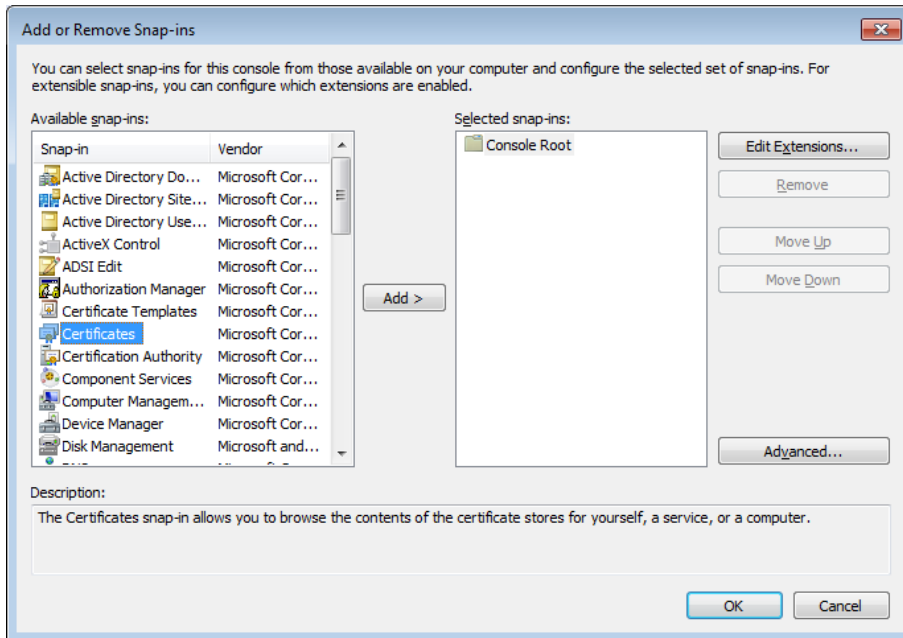
Type the Windows Key + R. A new dialog is shown. Type "mmc" and press Enter.



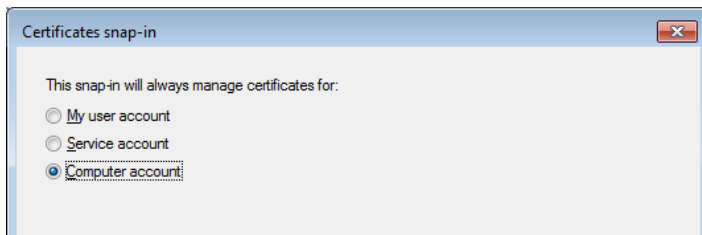
Open the menu File -> Add/Remove Snap-in



Select "certificates" and press "Add >"

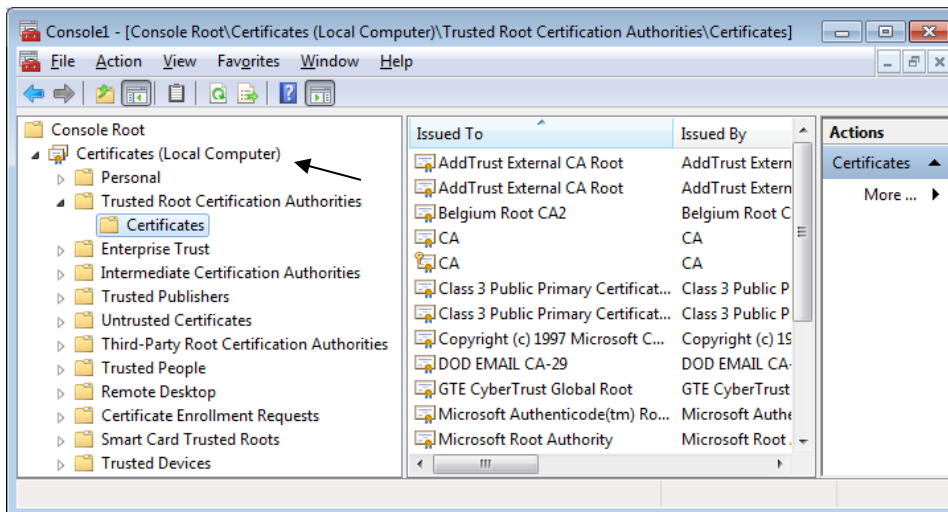


Select "Computer account"



The certificate store dialog appears. Open the "Trusted Root Certification Authorities" folder and check at the right that the certificate appears.

Please pay attention to the mention "Local computer"





### ***Install asp.net if it is not already installed***

The procedure to install asp.net on IIS is described here:

<http://technet.microsoft.com/en-US/us-en/library/hh831475.aspx>

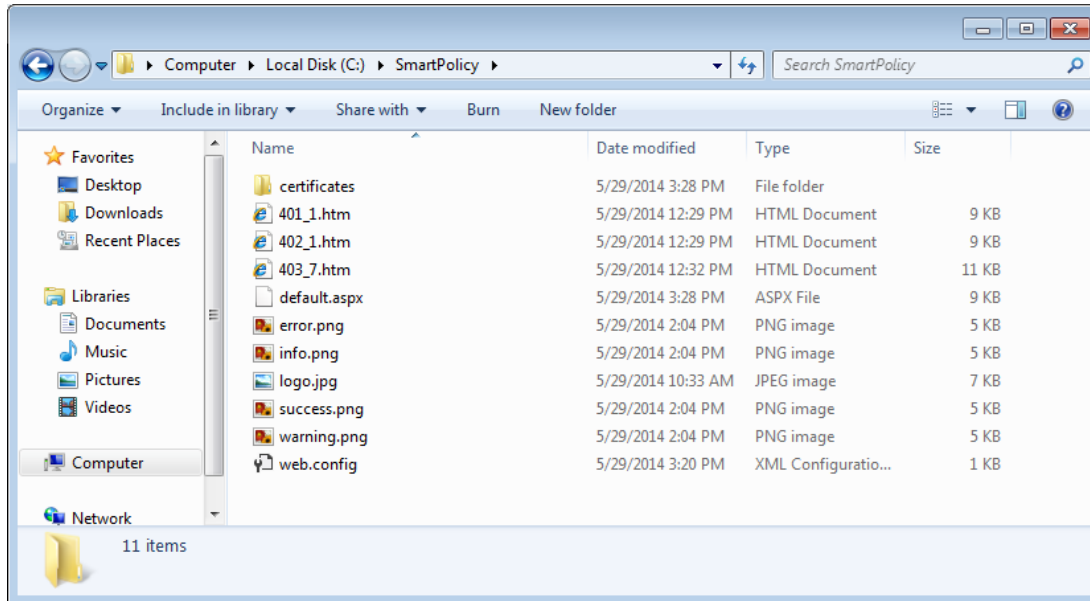
The following command installs the components missing in a default IIS installation:

```
Start /w pkgmgr /iu:IIS-WebServerRole;IIS-WebServer;IIS-CommonHttpFeatures;IIS-StaticContent;IIS-DefaultDocument;IIS-DirectoryBrowsing;IIS-HttpErrors;IIS-ApplicationDevelopment;IIS-ASPNET;IIS-NetFxExtensibility;IIS-ISAPIExtensions;IIS-ISAPIFilter;IIS-HealthAndDiagnostics;IIS-HttpLogging;IIS-LoggingLibraries;IIS-RequestMonitor;IIS-Security;IIS-RequestFiltering;IIS-HttpCompressionStatic;IIS-WebServerManagementTools;IIS-ManagementConsole;WAS-WindowsActivationService;WAS-ProcessModel;WAS-NetFxEnvironment;WAS-ConfigurationAPI
```

## Installation

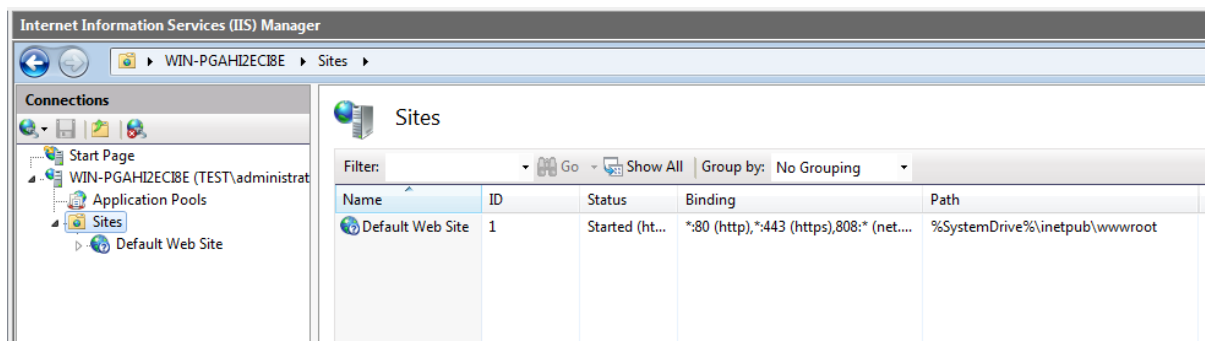
Smart Policy Web collector can be installed on a standalone website OR in a virtual directory.

Each procedure requires that the Smart Policy files are copied to a directory:

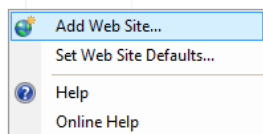


### 1a New website installation

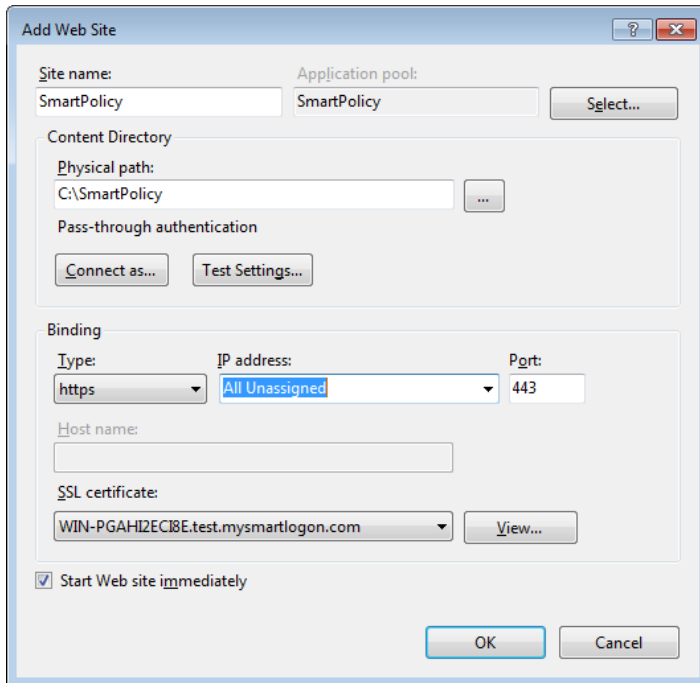
To create a new website, open the IIS Console and navigate to "Sites"



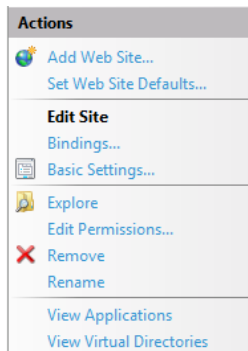
Right click and select "Add Web Site"



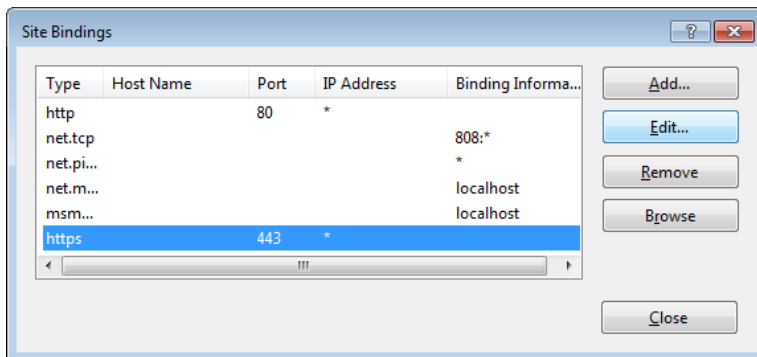
Specify the Site name, the Physical path to the directory you created with the Smart Policy files, select the binding type "https" and select the webserver SSL certificate.



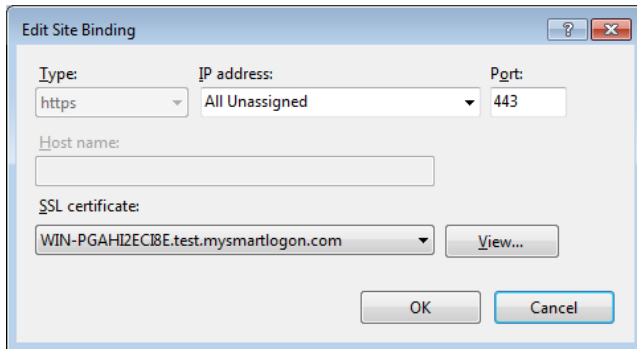
You can change the website certificate later by selecting your website and click on the right panel to "Bindings".



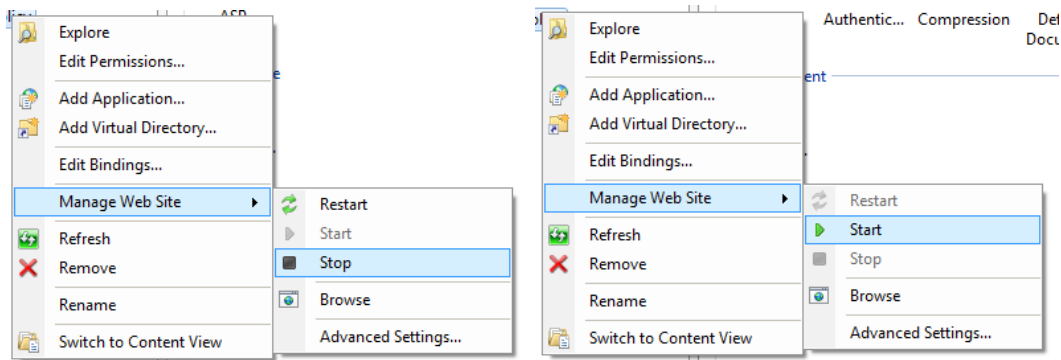
Select the "https" binding and select Edit.



Then change the SSL certificate.

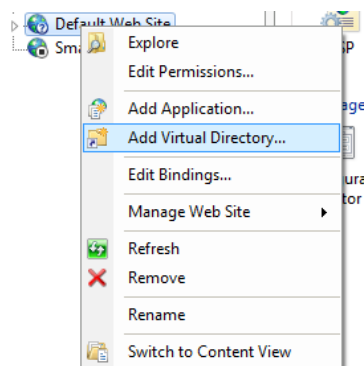


If the default site is already started, you have to stop it and start the new site manually.

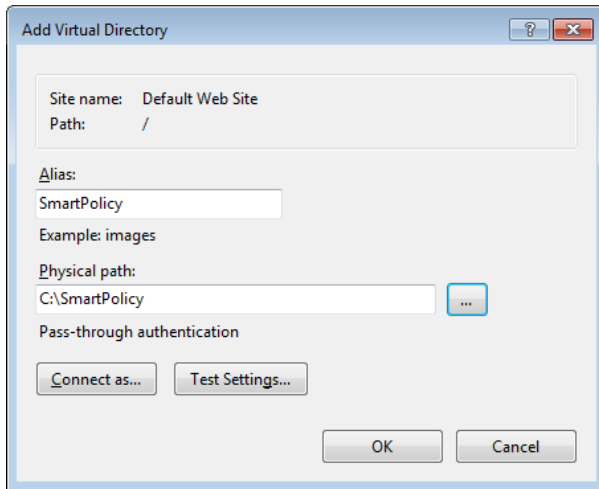


## 1b Virtual directory installation

To add a new virtual directory, right click on the website you want to edit. Select "Add Virtual Directory".



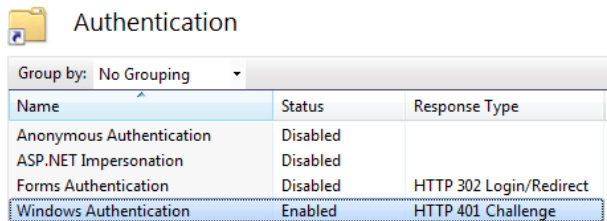
Enter the alias and select the directory where the smart policy files are stored.



## 2 Enable the Windows Authentication

In Features View, double-click Authentication.

Disable all authentication types except "Windows Authentication" which should be enabled.



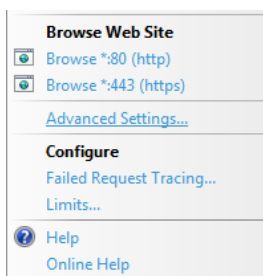
## 3 Enable kerberos authentication

By default, the application pool named "DefaultAppPool" runs under the account ApplicationPoolIdentity.

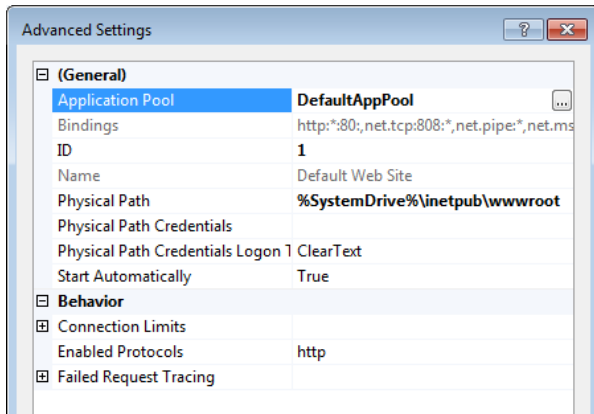
All authentication made on kerberos if the tool setspn.exe has not been run before WILL fail.

You can correct this by creating a new application pool running with the account "NetworkService" or you can change the account used in the default application pool.

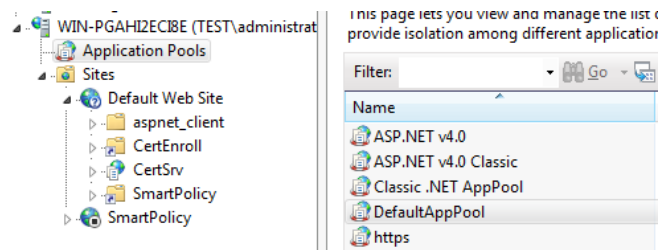
To determine the application pool used, go to "Advanced settings" for the website.



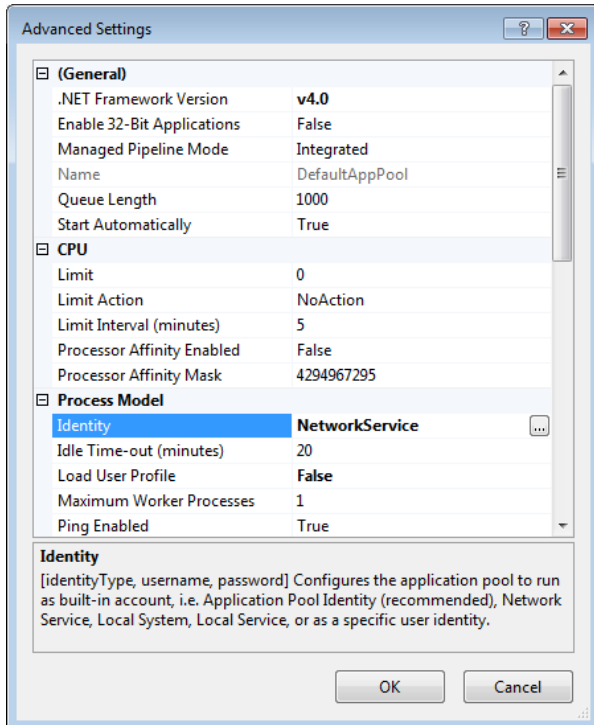
The application pool used in this case is "DefaultAppPool"



To edit the account used in the application pool, select "Application Pools" and locate the application pool you want to edit.



Click on "Advanced settings" and locate the entry named "Identity".



You can change it to "NetworkService" to solve this issue.


## 4 Configure the SSL settings

Open the SSL Settings for the website



SSL Settings

Set the "Require SSL" checkbox and select "Require" for the client certificates.

 **SSL Settings**  
This page lets you modify the SSL settings for the content of a Web site or application.  
 Require SSL  
Client certificates:  
 Ignore  
 Accept  
 Require

Note : to determine if the website is correctly installed, you can temporarily select "Accept".

## User workflow

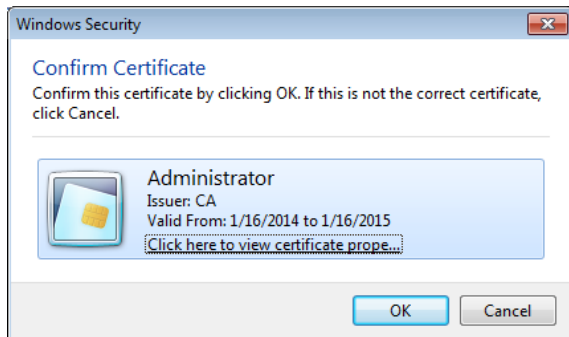
---

Enter the URL you configured previously. Typically <https://webserver> if you created a new website or <https://webserver/SmartPolicy> if you created a virtual directory.

The browser can issue a warning if the webserver's certificate is not trusted.

Then the browser shows a dialog to ask the user to select a certificate. If the user's computer is correctly configured, the smart card certificate should be shown.

Press OK

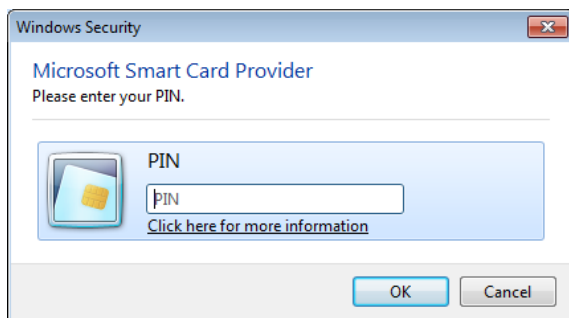


If the smart card was not inserted in the reader, a dialog may be shown to ask for the insertion.

**Warning:** when this dialog is shown, it can be hidden by the Internet Explorer Window.



The PIN should be asked by the browser. The dialog may not be shown if it has been asked previously and if the PIN has been cached.

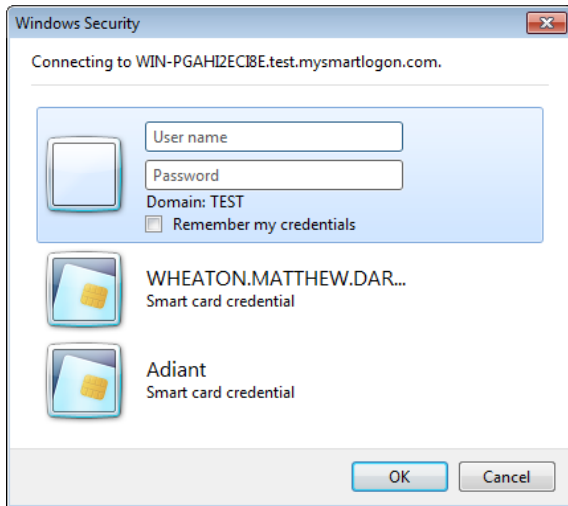


At this moment, the SSL connection should be established.

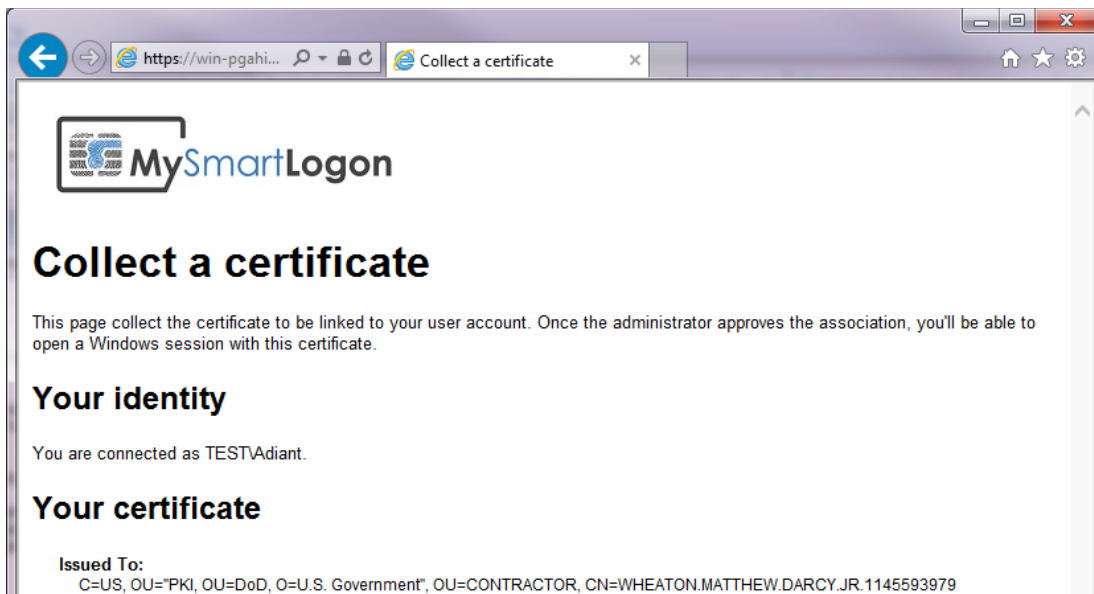
The browser then authenticates the user. The authentication may be hidden if the SSO is active or a dialog asking for a user password will be shown.

In this case, enter the login / password. Do not select the smart card certificate if the certificate has not been already assigned to the user. The authentication won't work.

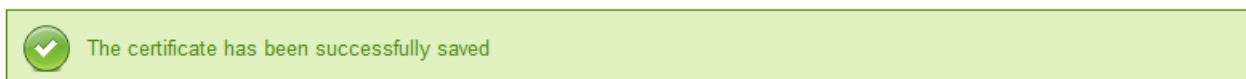




The Smart Policy Web Collector interface will be displayed.



Check the box and click on Confirm. A confirmation will be shown.



## ***Troubleshooting***

---

An [article published on msdn](#) describes a solution for the most common problems related to the client certificate authentication.

If Smart Policy detects a problem related to a client certificate authentication, it displays the following page:

### ***HTTP Error 403.7 - The client certificate was missing or unrecognized***

#### **Message :**

The page you are attempting to access requires your browser to have a Secure Sockets Layer (SSL) client certificate that the Web server recognizes.

#### **Cause :**

- No certificate was sent to the webserver
- Or a certificate was sent to the webserver and the webserver rejected it.

#### **Solution :**

You **MUST** close your browser before any other authentication attempt to force a new SSL connection.

If the browser prompted for a certificate and the dialog has not been cancelled that means that a certificate has been sent to the webserver.

#### **To make appear the dialog :**

- Check that the policy "don't prompt for client certificate selection when no certificate or only one certificate exists" is disabled. It can be found in the custom "security level" settings for a internet/intranet zone

#### **To add the smart card certificate to the dialog :**

- Check that the smart card is present
- Check that the smart card certificate is found by the browser. It should be present in the "Personal" folder on the user certificate store (certmgr.msc) If it is not present, check that the "certificate propagation service" is running
- Check that the smart card certificate is trusted by the browser Double click on the certificate found in the previous step Open the certificate properties, select the tab "certification path" and search for the label "the certificate is ok"

#### **To check that the smart card certificate is trusted by the webserver :**

- Check that the root certificate which signed the smart card certificate is trusted on the webserver. Extract the root certificate by double clicking on it on the "certification path" of the smart card certificate. Check its presence on the webserver in the folder "trusted root certification authorities" in the "computer certificate store" (and not in the "user certificate store").

#### **More information :**

<http://support.microsoft.com/kb/186812>

The certificate dialog can be hidden if the "Don't prompt for client certificate selection when no certificate or only one certificate exists" is enabled. To disable it, select the zone where the website is located and edit the level of the zone by pressing "Custom Level".

